RACHELE R. BYRD (190634)
byrd@whafh.com
BRITTANY N. DEJONG (258766)
dejong@whafh.com
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599

MATTHEW M. GUINEY (*pro hac vice forthcoming*)
guiney@whafh.com
LYDIA KEANEY REYNOLDS (*pro hac vice forthcoming*)
reynolds@whafh.com
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
270 Madison Avenue
New York, NY 10016
Telephone: 212/545-4600
Facsimile: 212/545-4677

Attorneys for Plaintiff

[Additional counsel appear on signature page]

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

KRISTEN HARTMANN, individually and on behalf of all others similarly situated,

Plaintiff,

v.

ZOOM VIDEO COMMUNICATIONS, INC.

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Kristen Hartmann ("Plaintiff"), individually and on behalf of all other similarly situated individuals, hereby alleges upon personal knowledge of the facts respectively pertaining to her own actions, and upon information and belief as to all other matters, by and through her undersigned counsel, and brings this Class Action Complaint against defendant Zoom Video Communications, Inc. ("Zoom" or "Defendant").

NATURE OF THE ACTION

1. In the space of months – which has accelerated rapidly due to the current COVID-19 pandemic – Zoom has exploded on to the videoconferencing stage, going from niche company to major platform for companies and individuals alike.

2. The most significant of these is Zoom Meetings, a product that combines live videoconferencing, chat, and desktop collaboration. Zoom prominently advertises that Zoom Meetings can be "secure[d]…with end-to-end encryption."[1]

3. End-to-end encryption (or "E2EE") is:

> [A] system of communication where the only people who can read the messages are the people communicating. No eavesdropper can access the cryptographic keys needed to decrypt the conversation—not even a company that runs the messaging service.[2]

4. E2EE is a valuable service to consumers, who will pay more on the understanding that their communication is entirely secure from outside view, including from the view of the company that owns and operates the platform (namely, Zoom itself).

5. However, on March 31, 2020, The Intercept first reported that Zoom Meetings is not, in fact, actually end-to-end encrypted.[3] Instead, Zoom uses a form of encryption called "transport encryption" and thus "the Zoom service itself can access the unencrypted video and

---

[1] ZOOM, https://zoom.us/security (last visited Apr. 15, 2020).

[2] Andy Greenberg, *Hacker Lexicon: What is End-to-End Encryption*, WIRED, https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/ (last visited Apr. 15, 2020).

[3] *See* Micah Lee & Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing*, THE INTERCEPT (Mar. 31, 2020, 1:00 AM), https://theintercept.com/2020/03/31/zoom-meeting-encryption/ (last visited Apr. 15, 2020).

audio content of Zoom meetings."[4]

6. Further, Zoom admitted as much to The Intercept, stating, "Currently, it is not possible to enable E2E encryption for Zoom video meetings."[5] Also, "[W]e recognize that there is a discrepancy between the commonly accepted definition of end-to-end encryption and how we were using it."[6]

7. Zoom apparently has not implemented E2EE – in spite of active advertising to the contrary – at least in part in order to collect and share information with advertisers, including "the content contained in cloud recordings, and instant messages, files, [and] whiteboards"[7] that are part of Zoom Meetings between users.

8. While Zoom has since updated its privacy policy to state that "Zoom does not sell customer content to anyone or use it for any advertising purposes," it continues to prominently advertise both on its website and within the Zoom Meetings platform that it utilizes E2EE functionality, even as it has publicly commented that it is unable to do so.[8]

9. Plaintiff, individually and on behalf of similarly situated consumers, seeks to recover damages, equitable relief, including injunctive relief in the form of corrected advertising and a corrective campaign to educate consumers, restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

PARTIES

10. Plaintiff Kristen Hartmann is a natural person residing in Montgomery County, Maryland.

---

[4] *Id.*

[5] *Id.*

[6] Oded Gal, *The Facts Around Zoom and Encryption for Meetings/Webinars*, ZOOM BLOG (Apr. 1, 2020), https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/ (last visited Apr. 15, 2020).

[7] Kate Cox, *Zoom's privacy problems are growing as platform explodes in popularity*, ARSTECHNICA (Mar. 31, 2020, 12:12 PM), https://arstechnica.com/tech-policy/2020/03/zooms-privacy-problems-are-growing-as-platform-explodes-in-popularity/ (last visited Apr. 15, 2020).

[8] *Id.*

11. On or about April 23, 2019, Plaintiff purchased a "Zoom Pro" monthly account for her own personal use, for which she pays $14.99 per month. Plaintiff purchased her account having seen advertising that Zoom Meetings were equipped with E2EE technology, which was a feature that she valued and for which she was willing to pay a premium. Further, periodically during Zoom Meetings calls, Plaintiff would "check" to ensure the calls were E2EE by hovering her cursor over the green lock icon in the application. The icon would then show text indicating active E2EE. Had Plaintiff known that Zoom Meetings were not actually end-to-end encrypted, she would not have paid for a Zoom Pro subscription, or she would have paid less for it.

12. Defendant Zoom Video Communications is a Delaware corporation with its principal place of business at 55 Almaden Blvd., San Jose, California.

JURISDICTION AND VENUE

13. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) ("The Class Action Fairness Act") because sufficient diversity of citizenship exists between the parties to this action, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and there are 100 or more members of the Class.

14. This Court has personal jurisdiction over Defendant, which has its principal place of business in this district and which is authorized to and regularly conducts business in the Northern District of California.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Defendant is a corporation with its principal place of business within this District, and a substantial part of the events and omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

16. Zoom was founded in 2011, and it rapidly gained a reputation as a videoconferencing disruptor with good features and attractive, consumer-friendly pricing.[9] Even

[9] *See* David S. Maldow, Esq., *Zoom's Full Feature UME Videoconferencing Platform Exceeds Expectations*, TELEPRESENCE OPTIONS (Jan. 27, 2013), http://www.telepresenceoptions.com/2013/01/zooms_full_featured_ume_videoc/ (last visited Apr. 15, 2020).

in early reviews, such as those in 2013, Zoom actively touted its security credentials, informing reviewers that it could "meet industry security expectations."[10]

17. E2EE has become an important, valuable service that consumers actively seek out when looking for platforms in order to communicate. For example, when the incredibly popular messaging application WhatsApp implemented E2EE in 2016, industry observers noted:

> End-to-end encryption means the content of communications are not stored in plaintext on WhatsApp's servers. Nor is the company able to decrypt users' messages to access them since it does not hold the encryption keys. So WhatsApp will be unable to be compelled to hand over messaging data — even if served with a warrant by authorities demanding access.
>
> While the WhatsApp news may seem timely in light of the recent high-profile battle between Apple and the FBI over an encrypted iPhone, the company has in fact been implementing encryption since 2013, the year NSA whistleblower Edward Snowden triggered a global privacy storm by revealing the extent of government mass surveillance programs.[11]

18. Increasingly, E2EE is becoming an industry standard expectation for communication technology. Facebook announced in March 2019 that it would move all three of its messaging platforms (including WhatsApp) to E2EE.[12] Similarly, Apple says of its data security: "iCloud is built with industry-standard security technologies, employs strict policies to protect your information, and is leading the industry by adopting privacy-preserving technologies like end-to-end encryption for your data."[13]

19. Competitor platforms Webex and GoToMeeting both either automatically utilize

---

[10] *Id.*

[11] Natasha Lomas, *WhatsApp completes end-to-end encryption rollout*, TECHCRUNCH (Apr. 5, 2016, 8:40 AM), https://techcrunch.com/2016/04/05/whatsapp-completes-end-to-end-encryption-rollout/ (last visited Apr. 15, 2020).

[12] Nicole Perlroth, *What Is End-to-End Encryption? Another Bull's Eye on Big Tech*,, NEW YORK TIMES (Nov. 19, 2019), https://www.nytimes.com/2019/11/19/technology/end-to-end-encryption.html (last visited Apr. 15, 2020).

[13] *iCloud Security Update*, APPLE, https://support.apple.com/en-us/HT202303 (last visited Apr. 15, 2020).

E2EE or offer hosts the option of E2EE as part of their standard platform.[14]

20. As a result, Zoom is and has been aware that E2EE is a valuable service that consumers will both pay for and have increasingly come to expect as part of their online communication choices.

21. With this in mind, Zoom appears to have first added explicit representations that it had E2EE functionality at least as early as 2019. For example, Zoom made the following representations in 2019 and early 2020:

> Zoom exceeds a high standard for data privacy and protection so your information stays safe and secure. Zoom is certified and compliant with the EU-U.S. Privacy Shield Framework as well as the following measures:
> . . .
> - End-to-end-encryption for desktop and mobile devices[15]

22. Similarly, on Zoom's own website, the following representations were prominently shown in the "Security at Zoom" page:

> We take security seriously and we are proud to exceed industry standards when it comes to your organization's communications . . . .
> . . .
> The following in-meeting security capabilities are available to the meeting host:
> - Secure a meeting with end-to-end encryption
> . . .
> Zoom's solution and security architecture provides end-to-end encryption and meeting access controls so data in transit cannot be intercepted. [16]

23. Security whitepapers are authoritative guides that major online platforms and

---

[14] *What Does End-to-End Encryption Do?*, CISCO WEBEX HELP CENTER, https://help.webex.com/en-us/WBX44739/What-Does-End-to-End-Encryption-Do (last visited Apr. 15, 2020) and *White Paper: Security*, GOTOMEETING, https://logmeincdn.azureedge.net/gotomeetingmedia/-/media/pdfs/gotomeeting-security-white-paper-286395.pdf, at 6 (last visited Apr. 15, 2020).

[15] Zoom, *Executive Summary*, https://www.neha.org/sites/default/files/Zoom%20Executive%20Summary%202019.pdf, at 10 (last visited Apr. 15, 2020).

[16] INTERNET ARCHIVE WAYBACK MACHINE, *Security at Zoom*, (March 22, 2020), http://web.archive.org/web/20200322145328/https://zoom.us/security (last visited Apr. 15, 2020).

institutions use to discuss their security credentials to their users and consumers. Zoom also prominently linked (and continues to link) to a "Security Whitepaper" on its "Security at Zoom" page which states the following:

> Role-based user security
> The following pre-meeting security capabilities are available to the meeting host:
> - Enable an end-to-end (E2E) encrypted meeting[17]

24. Additionally, during Zoom Meetings, hovering your cursor over the green lock at the top left corner of the application would show the text "Zoom is using an end to end encrypted connection."[18] Zoom has since changed this text to simply say that the session is encrypted.

25. On March 31, 2020, The Intercept published an article stating publicly that Zoom Meetings and Zoom's other audio and video functionality did not, in fact, support E2EE. The article stated:

> In Zoom's white paper, there is a list of "pre-meeting security capabilities" that are available to the meeting host that starts with "Enable an end-to-end (E2E) encrypted meeting." Later in the white paper, it lists "Secure a meeting with E2E encryption" as an "in-meeting security capability" that's available to meeting hosts. When a host starts a meeting with the "Require Encryption for 3rd Party Endpoints" setting enabled, participants see a green padlock that says, "Zoom is using an end to end encrypted connection" when they mouse over it.
>
> But when reached for comment about whether video meetings are actually end-to-end encrypted, a Zoom spokesperson wrote, "Currently, it is not possible to enable E2E encryption for Zoom video meetings. Zoom video meetings use a combination of TCP and UDP. TCP connections are made using TLS and UDP connections are encrypted with AES using a key negotiated over a TLS connection."[19]

---

[17] INTERNET ARCHIVE WAYBACK MACHINE, *Zoom Security Guide*, (March 31, 2020), http://web.archive.org/web/20200331082306/https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf (last visited Apr. 15, 2020).

[18] *See, e.g.*, Bill Marczak & John Scott-Railton, *Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings*, THE CITIZEN LAB (Apr. 3, 2020), https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/ (last visited Apr. 15, 2020).

[19] Micah Lee & Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing*, THE INTERCEPT (Mar. 31, 2020, 1:00 AM), https://theintercept.com/2020/03/31/zoom-meeting-encryption/ (last visited Apr. 15, 2020).

26. This is particularly important because it means that Zoom itself is able to access the audio and video content of Zoom meetings, including to potentially mine them for saleable marketing data. The article explained this in detail:

> The encryption that Zoom uses to protect meetings is TLS, the same technology that web servers use to secure HTTPS websites. This means that the connection between the Zoom app running on a user's computer or phone and Zoom's server is encrypted in the same way the connection between your web browser and this article . . . is encrypted. This is known as transport encryption, which is different from end-to-end encryption because the Zoom service itself can access the unencrypted video and audio content of Zoom meetings. So when you have a Zoom meeting, the video and audio content will stay private from anyone spying on your Wi-Fi, but it won't stay private from the company.[20]

27. Indeed, Zoom's security practices drew national attention on March 26, 2020 (five days before The Intercept broke the news of Zoom's deceptive E2EE marketing) with the revelation that Zoom sends user data to Facebook which can help Facebook determine advertising information for use in selling its own targeted advertising.[21]

28. The article further elaborated on how Zoom's video encryption does not match those of others in the industry, stating:

> Matthew Green, a cryptographer and computer science professor at Johns Hopkins University, points out that group video conferencing is difficult to encrypt end to end. That's because the service provider needs to detect who is talking to act like a switchboard, which allows it to only send a high-resolution videostream from the person who is talking at the moment, or who a user selects to the rest of the group, and to send low-resolution videostreams of other participants. This type of optimization is much easier if the service provider can see everything because it's unencrypted.
>
> "If it's all end-to-end encrypted, you need to add some extra mechanisms to make sure you can do that kind of 'who's talking' switch, and you can do it in a way that doesn't leak a lot of information. You have to push that logic out to the endpoints," he told The Intercept. This isn't impossible, though, Green said, as

---

[20] *Id.*

[21] *See* Joseph Cox, *Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account*, MOTHERBOARD: TECH BY VICE (Mar. 26, 2020, 5:00 AM) https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account (last visited Apr. 15, 2020).

> demonstrated by Apple's FaceTime, which allows group video conferencing that's end-to-end encrypted. "It's doable. It's just not easy."
>
> "They're a little bit fuzzy about what's end-to-end encrypted," Green said of Zoom. **"I think they're doing this in a slightly dishonest way. It would be nice if they just came clean."**
>
> The only feature of Zoom that does appear to be end-to-end encrypted is in-meeting text chat.[22]

(Emphasis added).

29. Zoom's own response on April 1, 2020 (the day after The Intercept's article) made it clear that Zoom both knew that it did not use the industry-accepted definition of E2EE and had made a conscious decision to use the term "end-to-end" anyway:

> In light of recent interest in our encryption practices, we want to start by apologizing for the confusion we have caused by incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption. **Zoom has always strived to use encryption to protect content in as many scenarios as possible, and in that spirit, we used the term end-to-end encryption**. While we never intended to deceive any of our customers, **we recognize that there is a discrepancy between the commonly accepted definition of end-to-end encryption and how we were using it**.[23]

(Emphasis added)

30. However, researchers and experts have pointed out that even with this blog post intended to address concerns over Zoom's security representations, Zoom still has not publicly described the exact nature of its video encryption, nor has it stated what type of encryption it does employ.[24]

31. Since the publication of The Intercept article whose allegations are at the heart of this complaint, numerous other issues have come to light showing that Zoom's security practices have been at best sloppy and at worst malicious and unsafe in handling customer data, including routing meetings through Chinese servers (which are closely scrutinized by the Chinese government), using an installer for the application which can allow access to a computer's

---

[22] Lee & Grauer, *supra* note 19.

[23] Gal, *supra* note 6.

[24] *See* Marczak & Scott-Railton, *supra* note 18.

microphone and camera without user permission, and substandard login procedures which can allow malicious actors to randomly access Zoom Meetings even if not invited.[25]

32. While the allegations regarding Zoom misrepresenting E2EE are at the heart of this complaint, taken together, these vulnerabilities and security flaws in Zoom's software and routing reveal a company that actively misrepresented the security and functionality of its products and services to sell them to consumers in a highly competitive marketplace. As a result, though, Plaintiff and Class members paid an inflated price for a service which did not function as explicitly represented by Zoom.

CLASS ACTION ALLEGATIONS

33. Plaintiff brings this action on behalf of herself and as a class action under Federal Rules of Civil Procedure, rule ("Rule(s)") 23(a), (b)(2), and (b)(3), seeking damages and equitable relief on behalf of the following nationwide Class:

> All persons residing in the United States who purchased a paid Zoom account for the purpose of using Zoom Meetings.

34. Plaintiff also brings this action on behalf of herself and as a class action under Rule 23(a), (b)(2), and (b)(3), seeking damages and equitable relief on behalf of the following Subclass:

> All persons residing in the State of Maryland who purchased a paid Zoom account for the purpose of using Zoom Meetings.

35. Excluded from the Class are Defendant; any parent, affiliate, or subsidiary of Defendant; any entity in which Defendant has a controlling interest; any of Defendant's officers or directors; and any successor or assign of Defendant. Also excluded are any Judge or court personnel assigned to this case and members of their immediate families.

36. Plaintiff hereby reserves the right to amend or modify the class definition with

[25] *See, e.g.*, Brian Feldman, *Is It Safe to Use Zoom*?, NEW YORK MAGAZINE (Apr. 9, 2020) https://nymag.com/intelligencer/2020/04/the-zoom-app-has-a-lot-of-security-problems.html (last visited Apr. 15, 2020).

greater specificity or division after having had an opportunity to conduct discovery.

37. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the Class and Subclass are so numerous that joinder of all members is impracticable. While Plaintiffs do not know the exact number of the members of the Class or Subclass, Plaintiffs believe it contains at least tens of thousands of people. The exact number of Class and Subclass members are known to Defendant through billing and profile records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, social media, and/or published notice.

38. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirements, common questions of law and fact exist as to all members of the Class and Subclass, and predominate over any questions affecting individual Class and Subclass members. Such questions of law and fact common to the Class and Subclass include, but are not limited to:

a. Whether Defendant represented that Zoom Meetings had E2EE capability that it did not, in fact, contain;

b. Whether Defendant knew its representations about E2EE capability were false, misleading, and/or deceptive;

c. Whether Defendant intentionally misled customers about its E2EE capability for Zoom Meetings;

d. Whether Defendant engaged in the wrongful conduct alleged herein;

e. Whether Defendants' conduct constituted unfair or deceptive trade practices;

f. Whether Plaintiff and Class members were injured and suffered damages or other losses because of Defendant's fraudulent conduct; and

g. Whether Plaintiff and Class members are entitled to relief, including equitable relief.

39. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of the claims of the members of the Class and Subclass. Plaintiff is a consumer who purchased a paid Zoom for an account in order to conduct meetings which she understood to

be E2E encrypted. Plaintiff's damages and injuries are akin to those of other Class and Subclass members, and Plaintiff seeks relief consistent with the relief of the Class and Subclass members.

40. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class and Subclass because Plaintiff is a member of the Class and Subclass and is committed to pursuing this matter against Defendant to obtain relief for the Class and Subclass. Plaintiff has no conflicts of interest with the Class and Subclass members. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' and Subclass' interests. Plaintiff's claims arise out of the same common course of conduct giving rise to the claims of the other members of the Class and Subclass. Plaintiff's interests are coincident with, and not antagonistic to, those of the other members of the Class and Subclass.

41. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class and Subclass are relatively small compared to the burden and expense required to individually litigate their claims against Defendants, and, thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class and Subclass member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

42. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendants, through uniform conduct, acted or refused to act on grounds generally applicable to the Class and Subclass as a whole, making injunctive and declaratory

relief appropriate to the Class and Subclass as a whole.

43. Finally, all members of the proposed Class and Subclass are readily ascertainable. Defendant has access to customer payment and billing records that will show who is a Class and Subclass member.

FIRST CLAIM FOR RELIEF
Fraud
(By Plaintiff on Behalf of the Class and Subclass)

44. Plaintiff restates and realleges paragraphs 1 through 43 as if fully set forth herein.

45. Defendant made false and misleading statements about the characteristics of its videoconferencing services.

46. Defendant knows and has known that its statements were false and misleading, as evidenced by official statements issued by the CEO, referenced *supra*.

47. Defendant's representations about its videoconferencing services were intended to defraud its customers and potential customers in order to induce them to sign up for its services.

48. Plaintiff and the Class relied on Defendant's false and misleading statements in signing up for and paying for Defendant's services. E2EE encryption is a valuable part of Defendant's videoconferencing services, and Plaintiff had the right to rely on Defendant's statements that its videoconferencing services had E2EE functionality when purchasing Defendant's services.

49. Plaintiff suffered economic injury as a result of paying for Defendant's services.

SECOND CLAIM FOR RELIEF
Maryland Consumer Protection Act, Md. Commercial Law Code Ann. § 13-101, *et seq.*
(By Plaintiff on Behalf of the Maryland Subclass)

50. Plaintiff restates and realleges paragraphs 1 through 43 as if fully set forth herein.

51. Plaintiff and the Maryland Subclass are consumers within the meanings of Md. Commercial Law Code Ann. § 13-101(c).

52. Defendant's videoconferencing services are consumer services within the meaning of Md. Commercial Law Code Ann. § 13-101(d)(1).

53. Defendant represented that its videoconferencing services had characteristics which they did not, in fact, have.

54. Further, Defendant advertised or offered its services without intent to sell, lease, or rent them as offered.

55. Additionally, Defendant used deception, fraud, and misrepresentation in the sale of its videoconferencing services in that it advertised them as containing E2EE when it knew that they did not.

56. Defendant's representations of its services utilizing E2EE were intended to induce – and did, in fact, induce – Plaintiff and the Maryland Subclass to purchase Defendant's videoconferencing services.

57. Defendant is liable to Plaintiff and the Maryland Subclass for damages, including reasonable attorney's fees, as set forth in Md. Commercial Law Code Ann. § 13-408(a)-(b).

THIRD CLAIM FOR RELIEF
Unjust Enrichment
(By Plaintiff on Behalf of the Class and Subclass)

58. Plaintiff repeats the allegations contained in paragraphs 1 through 43 as if fully set forth herein.

59. Plaintiff brings this claim individually and on behalf of the members of the Class and Subclass against Defendant.

60. Plaintiff and the other members of the Class and Subclass conferred benefits on Defendant by purchasing Defendant's videoconferencing services.

61. Defendant has been unjustly enriched by retaining the revenues derived from Plaintiff's and the other members of the Class' and Subclass' purchases of its videoconferencing services. Retention of the monies under these circumstances is unjust and inequitable because Defendant's representations were misleading to consumers, which caused injuries to Plaintiff and the other members of the Class and Subclass because they would not have purchased the videoconferencing services if the true facts had been known.

62. Because Defendant's retention of the non-gratuitous benefits conferred on it by Plaintiff and the other members of the Class and Subclass is unjust and inequitable, Defendant must pay restitution to Plaintiff and the other members of the Class and Subclass for its unjust

enrichment, as ordered by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class and Subclass, respectfully seeks from the Court the following relief:

a. Certification of the Class and Subclass as requested herein;

b. Appointment of Plaintiff as Class Representative and her undersigned counsel as Class Counsel;

c. An order awarding Plaintiff and members of the proposed Class and Subclass damages;

d. An order awarding Plaintiff and members of the proposed Class and Subclass equitable, injunctive and declaratory relief, including the enjoining of Defendant's conduct at issue herein and Defendant's continuation of its unlawful business practices as alleged herein;

e. An order declaring that Defendant's acts and practices as alleged herein are fraudulent;

f. An order awarding Plaintiff and members of the proposed Class and Subclass pre-judgment and post-judgment interest as permitted by law;

g. An order awarding Plaintiff and members of the proposed Class and Subclass reasonable attorney fees and costs of suit, including expert witness fees; and

h. An order awarding Plaintiff and members of the proposed Class and Subclass any further relief the Court deems proper.

JURY DEMAND

Plaintiff, on behalf of herself and the Class and Subclass, hereby demands a trial by jury on all issues so triable pursuant to Rule 38.

DATED: April 15, 2020

Respectfully submitted,

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP

/s/ Rachele R. Byrd
RACHELE R. BYRD

RACHELE R. BYRD
byrd@whafh.com
BRITTANY N. DEJONG
dejong@whafh.com
750 B Street, Suite 1820
San Diego, California
Telephone: 619/239-4599
Facsimile: 619/234-4599

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
MATTHEW M. GUINEY
guiney@whafh.com
LYDIA KEANEY REYNOLDS
reynolds@whafh.com
270 Madison Avenue
New York, New York 10016
Telephone: 212/545-4600
Facsimile: 212/545-4653

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
CARL MALMSTROM (*pro hac vice forthcoming*)
malmstrom@whafh.com
111 W. Jackson St., Suite 1700
Chicago, IL 60604
Telephone: 312/984-0000
Facsimile: 212/545-4653

Attorneys for Plaintiff

ZOOM/26397